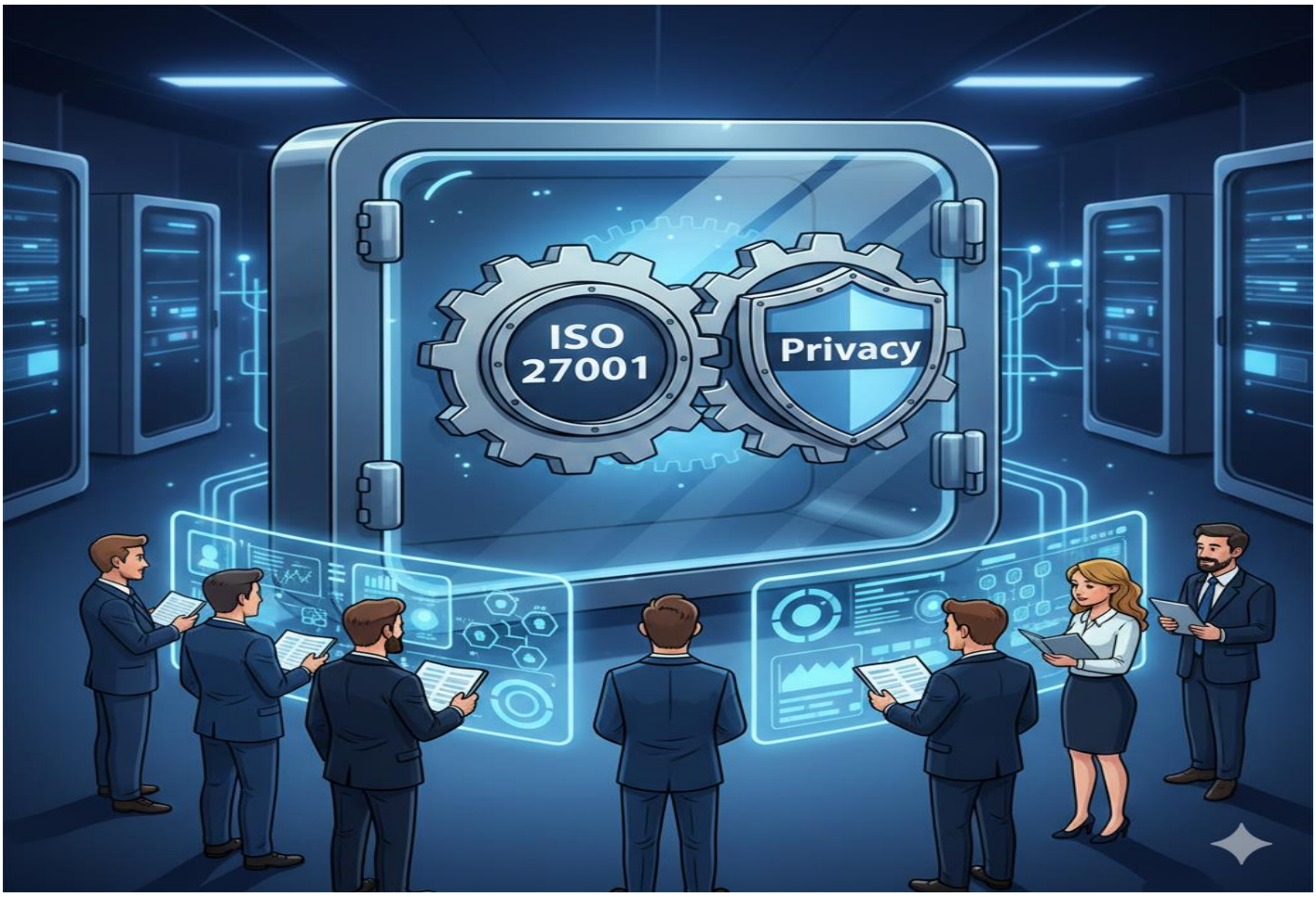
Roma, 15/01/2026

NEWSLETTER

"Numero 01/2026"

Notiziario del Responsabile della Protezione dei Dati personali della Difesa

- **Federprivacy:** ISO 27001 e Privacy: un binomio strategico per la *governance* del dato (Federprivacy). *(**Fonte: Federprivacy – articolo del 10 dicembre 2025**)*;
- **Garante privacy:** Garante privacy. Tra AI e dati personali: la sfida di una democrazia digitale secondo Ginevra Cerrina Feroni. *(**Fonte: Garante privacy – Intervista a Ginevra Cerrina Feroni, Vice presidente del Garante per la protezione dei dati personali AssociazioneCittadinanzaDigitale.org, 10 dicembre 2025**)*;
- **Federprivacy:** *Social media online* la guida aggiornata del Garante privacy *(**Fonte: Federprivacy – articolo del 18 novembre 2025**)*.



ISO 27001 e Privacy un binomio strategico per la *governance* del dato

Nel pieno della trasformazione digitale, la protezione delle informazioni non rappresenta più un elemento accessorio, bensì una condizione imprescindibile per qualunque organizzazione che voglia garantire affidabilità, continuità operativa e rispetto delle normative in materia di protezione dei dati personali.
In questo scenario, la ISO/IEC 27001 si conferma uno degli standard internazionali più solidi per strutturare un sistema di gestione della sicurezza delle informazioni fondato sui principi di integrità, riservatezza e disponibilità. La sua adozione costituisce un fattore abilitante sia per il rispetto del Regolamento (UE) 2016/679 (GDPR), che richiede misure tecniche e organizzative adeguate, proporzionate ai rischi e costantemente aggiornate, sia delle ulteriori normative poste a tutela dei dati personali.
La forza della ISO 27001 risiede nell'approccio metodico basato sulla valutazione del rischio e sulla definizione di controlli puntuali, che permettono di affrontare le minacce in maniera preventiva e non meramente reattiva. Questo impianto si intreccia con il principio di *accountability*, cardine del GDPR: non è sufficiente proteggere i dati personali, occorre poter dimostrare in modo chiaro, documentato e verificabile l'efficacia e l'adeguatezza delle misure adottate. In questo senso, la certificazione ISO 27001 assume un valore probatorio significativo, perché attesta la maturità del sistema di *governance* della sicurezza e la capacità dell'organizzazione di presidiare processi, ruoli e responsabilità in modo coerente e trasparente.
La relazione tra sicurezza informatica e tutela dei diritti fondamentali trova una suggestiva sintesi nelle parole di Stefano Rodotà, quando ricordava la necessità di tutelare il "corpo elettronico" delle persone. L'affermazione evidenzia un concetto spesso sottovalutato: proteggere le informazioni non significa esclusivamente custodire dati, ma salvaguardare la libertà, la dignità e l'autodeterminazione digitale dell'individuo. Un sistema come la ISO 27001 non costituisce dunque un semplice presidio tecnico, bensì una componente essenziale della protezione della persona, intesa nella sua dimensione moderna e tecnologicamente mediata.

Un altro elemento di rilievo riguarda il principio del miglioramento continuo. La ISO 27001 non si limita a richiedere l'implementazione iniziale di politiche e controlli: impone una revisione costante dell'intero sistema, affinché rimanga efficiente a fronte di nuove minacce, innovazioni tecnologiche o significativi cambiamenti organizzativi. Tale impostazione rispecchia pienamente lo spirito del GDPR, che impone un adeguamento dinamico delle misure di sicurezza e una valutazione ricorrente dei rischi, in un contesto caratterizzato da crescente complessità e interconnessione.

In questo percorso, un ruolo determinante è svolto anche dai piani di *audit*, sia interni sia indipendenti. Lungi dall'essere meri adempimenti formali, gli *audit* rappresentano strumenti strategici per individuare vulnerabilità, migliorare i processi e alimentare una cultura della sicurezza realmente diffusa. Sono, inoltre, un elemento chiave per dimostrare alle autorità di controllo un approccio rigoroso e documentato alla gestione dei dati personali. È necessario, tuttavia, un cambiamento di prospettiva all'interno delle organizzazioni: gli *audit* devono essere percepiti non come interventi ispettivi, ma come momenti di crescita, volti a stimolare consapevolezza, responsabilizzazione e capacità di generare valore.

La convergenza tra ISO 27001 e GDPR, dunque, non è casuale: entrambe le normative si fondano su un impianto culturale che vede nella protezione del dato non un vincolo, ma un *driver* strategico di affidabilità, competitività e sostenibilità digitale. Le aziende che adottano tale visione contribuiscono in maniera sostanziale a un ecosistema più sicuro, trasparente e rispettoso dei diritti degli interessati.

Tra AI e dati personali la sfida di una democrazia digitale secondo Ginevra Cerrina Feroni

Intervista a Ginevra Cerrina Feroni, Vice presidente del Garante per la protezione dei dati personali *(AssociazioneCittadinanzaDigitale.org, 10 dicembre 2025).*

La protezione dei dati personali e la cittadinanza digitale sono diventati temi centrali in un Paese che sta vivendo una trasformazione digitale rapida e complessa. L'adozione di servizi digitali da parte della Pubblica amministrazione, l'uso crescente dell'intelligenza artificiale e la gestione di grandi volumi di informazioni personali richiedono non solo infrastrutture tecnologiche sicure, ma anche cittadini consapevoli dei propri diritti e strumenti adeguati per esercitarli.

In questo contesto, Ginevra Cerrina Feroni, Vice Presidente del Garante per la protezione dei dati personali, svolge un ruolo fondamentale nel promuovere la cultura della protezione dei dati, guidando iniziative di alfabetizzazione digitale e collaborando con scuole, associazioni civiche e istituzioni per garantire che l'innovazione tecnologica sia compatibile con i diritti e le libertà dei cittadini.

Abbiamo avuto l'opportunità di intervistarla per approfondire il livello di consapevolezza dei cittadini italiani, i rischi legati alla gestione dei dati personali, il ruolo delle istituzioni nella *governance* digitale e le sfide future per costruire una democrazia digitale inclusiva, sicura e responsabile.

Come valuta il livello di consapevolezza dei cittadini italiani in materia dì protezione dei dati personali, soprattutto quando interagiscono online con la Pubblica amministrazione e i servizi digitali?

Ogni interazione dei cittadini italiani con i servizi digitali, pubblici o privati, lascia tracce della vita digitale, spesso senza che gli utenti ne siano pienamente consapevoli. Dalla navigazione sui motori di ricerca alla consultazione dì una piattaforma della Pubblica amministrazione, fino all'interazione con strumenti di intelligenza artificiale, ogni gesto produce dati che possono rivelare informazioni personali. È un fenomeno quotidiano, invisibile, ma pervasivo: cediamo informazioni su noi stessi senza pensarci, non sempre comprendendo le implicazioni di queste condivisioni.

La consapevolezza digitale richiede quindi un approccio attento e responsabile: occorre cautela, controllo e conoscenza dei propri diritti. Non si tratta solo di saper usare strumenti tecnologici, ma di capire le conseguenze della nostra vita digitale e la responsabilità che comporta. Per questo è fondamentale promuovere una cultura digitale diffusa, capace di trasformare la consapevolezza individuale in partecipazione attiva e protezione reale dei dati. Oggi, purtroppo, una cultura di questo tipo non è ancora pienamente radicata, anche se l'impatto delle nuove tecnologie sulla vita quotidiana dei cittadini è evidente e crescente.

Ogni giorno ci troviamo davanti a scelte digitali che incidono profondamente sulla nostra privacy. Anche semplici azioni, come fornire dati per un servizio pubblico online*, possono avere conseguenze significative se non si è pienamente consapevoli dei rischi e delle garanzie. La sfida principale consiste quindi nel trasformare la consapevolezza, spesso superficiale o sporadica, in competenza solida e diffusa.*

Quali sono oggi, secondo lei, i principali rischi per i diritti dei cittadini nell'ambito della protezione dei dati personali, considerato il crescente ricorso da parte delle pubbliche amministrazioni e delle imprese a soluzioni digitali integrate e interconnesse?

Proteggere i diritti e le libertà nell'era digitale significa, in primo luogo, proteggere il dato personale. In un contesto sempre più datificato, i rischi si manifestano in forme diverse: la violazione della segretezza di chat e email, l'accesso improprio a conti correnti, la diffusione non autorizzata di foto e video. Nell'ambito della Pubblica amministrazione, i rischi assumono una dimensione ancora più critica, perché i dati gestiti riguardano servizi essenziali e informazioni altamente sensibili.

Un data breach *può avere conseguenze enormi, non solo dal punto di vista tecnologico, ma anche rispetto ai diritti dei cittadini.*

Le misure per ridurre questi rischi sono molteplici e devono integrarsi in un quadro complessivo di sicurezza. La centralizzazione sicura delle banche dati, l'uso di tecniche di anonimizzazione e di dati sintetici, il controllo rigoroso degli accessi e la cifratura dei sistemi rappresentano strumenti essenziali. È altrettanto importante mantenere aggiornati software *e dati, perché informazioni obsolete possono generare errori e vulnerabilità. Infine, il rispetto dei principi del GDPR, come la minimizzazione dei dati raccolti e la responsabilizzazione dei titolari del trattamento, rimane il fondamento della protezione dei cittadini.*

Oltre agli aspetti tecnici, la sfida riguarda anche la cultura della sicurezza e la consapevolezza dei cittadini. La protezione dei dati non è solo un obbligo normativo, ma un impegno civico: sapere come e dove i propri dati vengono trattati permette di ridurre i rischi e di utilizzare i servizi digitali in maniera più sicura e consapevole.

L'Associazione Cittadinanza Digitale promuove percorsi di alfabetizzazione informatica e consapevolezza digitale: secondo lei, quale ruolo possono e devono avere i cittadini nel governo della società digitale, e quali strumenti possono essere messi a disposizione per renderli davvero partecipi e protetti?

Il coinvolgimento dei cittadini parte dalla conoscenza. Non si può essere partecipi se non si comprende il tema. L'alfabetizzazione digitale deve quindi iniziare fin dall'infanzia, coinvolgendo scuole, famiglie e l'intera popolazione. Solo una cultura diffusa del dato permette una partecipazione consapevole, responsabile e rispettosa delle regole del la società digitale.

Le associazioni civiche e i comitati hanno un ruolo centrale nel creare un humus *culturale favorevole alla partecipazione digitale. È fondamentale non lasciare indietro le persone meno esperte o prive di strumenti tecnologici adeguati, come gli anziani, garantendo che tutti possano accedere ai servizi pubblici e comprendere i rischi e le opportunità degli strumenti digitali.*

La mancanza di un progetto nazionale coordinato rappresenta ancora oggi una lacuna: occorre costruire strategie integrate di alfabetizzazione digitale e sensibilizzazione civica, in grado di includere ogni fascia della popolazione e di creare cittadini consapevoli dei propri diritti e doveri. Solo un impegno strutturato e duraturo, con la collaborazione di scuole, associazioni e istituzioni, può trasformare la consapevolezza in partecipazione attiva e protezione reale dei dati.

Oggi la Pubblica amministrazione, in modo non sempre consapevole, sta adottando piattaforme che fanno uso di intelligenza artificiale anche per l'erogazione di servizi pubblici. Quali misure ritiene essenziali affinché gli algoritmi operino nel pieno rispetto dei diritti dei cittadini?

*L'intelligenza artificiale rappresenta una trasformazione sociale, economica e antropologica. La Pubblica amministrazione deve modernizzarsi e adottare piattaforme digitali avanzate, ma sempre nel rispetto dei principi costituzionali e della privacy. L'IA applicata ai servizi pubblici può migliorare efficienza, accessibilità e qualità, ma solo se progettata secondo il principio della "*dignity design*", costruita cioè nel rispetto della dignità dell'individuo.*

Gli algoritmi devono essere trasparenti, interpretabili e compatibili con il GDPR e con principi etici fondamentali. Solo così cittadini e personale pubblico possono percepire l'IA come un alleato, evitando il timore di una tecnologia incontrollabile. È essenziale accompagnare l'adozione di IA con percorsi di formazione, sensibilizzazione e monitoraggio continuo, per garantire un equilibrio tra innovazione e protezione dei diritti.

L'attenzione non riguarda solo la tecnologia, ma anche le persone che la gestiscono e la utilizzano. I sistemi devono essere progettati con la consapevolezza che ogni decisione automatizzata può avere conseguenze reali sulla vita dei cittadini, richiedendo supervisione costante e strumenti di governance *chiari e robusti.*

Come può essere rafforzata la collaborazione tra il Garante, le scuole e le associazioni civiche per promuovere una vera cultura della cittadinanza digitale, fondata sulla conoscenza dei propri diritti e doveri nel mondo online?

Fin dall'inizio del mandato, il Garante ha ritenuto prioritario diffondere la cultura della protezione dei dati in tutto il Paese. Sono state avviate iniziative capillari: privacy tour *nelle scuole, protocolli d'intesa con autorità locali, guide,* tutorial *e materiali didattici* online*. L'obiettivo è creare cittadini informati, consapevoli dei propri diritti e doveri e capaci di partecipare attivamente alla* governance *digitale.*

Questa collaborazione con scuole e associazioni civiche permette di includere tutte le fasce della popolazione, prevenire fenomeni di cyberbullismo e rafforzare la cittadinanza digitale. Ogni iniziativa, pur piccola, contribuisce alla costruzione di un humus culturale necessario per il futuro digitale del Paese, favorendo l'adozione di comportamenti responsabili e sicuri. Il coinvolgimento diretto dei giovani e dei minori è particolarmente strategico, perché costruisce consapevolezza fin dai primi contatti con il mondo digitale.

Negli ultimi anni il Garante ha assunto un ruolo cruciale nel dialogo con le istituzioni europee sul regolamento sull'intelligenza artificiale (AI *Act*). Quali opportunità e sfide individua in questo nuovo quadro normativo per garantire un uso etico e responsabile dei dati?

L'IA è un fenomeno globale che richiede un coordinamento internazionale. Il Garante ha svolto un ruolo chiave nel dialogo con le istituzioni europee, contribuendo alla definizione di linee guida armoniche tra AI Act *e GDPR. Decisioni italiane, come quel le su ChatGPT, hanno stimolato azioni simili in altri paesi, rafforzando la cooperazione europea e internazionale.*

Il nuovo quadro normativo offre opportunità concrete per promuovere un uso etico dei dati, garantendo che innovazione e protezione della privacy coesistano. La strada principale consiste nell'integrare questi principi nei servizi pubblici e privati, affinché i cittadini possano beneficiare delle potenzialità dell'IA senza compromettere propri diritti fondamentali. Questo richiede non solo strumenti normativi, ma anche educazione, formazione e cultura organizzativa diffusa.

In che modo il Garante può contribuire a sostenere l'innovazione nelle pubbliche amministrazioni e nelle imprese, evitando che la tutela dei dati sia percepita come un ostacolo, ma piuttosto come un fattore abilitante di fiducia e qualità dei servizi digitali?

Il ruolo del Garante non è sostenere direttamente l'innovazione, ma garantire che essa sia governata nel rispetto della protezione dei dati. Innovazione e tutela dei dati non sono finalità opposte, ma complementari. Attraverso pareri, linee guida e consulenze alle PA e alle imprese, il Garante assicura che i processi innovativi rispettino libertà e diritti fondamentali. Così la protezione dei dati diventa un fattore abilitante, capace di aumentare la fiducia nei servizi digitali e migliorare la qualità della vita dei cittadini, trasformando l'innovazione in uno strumento di progresso inclusivo e responsabile.

Guardando al futuro, quali competenze ritiene indispensabili per i funzionari pubblici e i decisori politici chiamati a governare processi digitali complessi e basati sui dati?

I funzionari pubblici e i decisori politici devono possedere competenze interdisciplinari: giuridiche, tecniche ed etiche. Solo una formazione integrata permette di assumere decisioni consapevoli, gestire dati complessi e governare la transizione digitale. La comprensione dell'importanza dei dati diventa quindi centrale nella leadership e nella gestione di processi digitali complessi, assicurando che innovazione e protezione dei cittadini procedano di pari passo.

Al contempo, occorre promuovere una cultura della responsabilità: coloro che prendono decisioni strategiche devono comprendere le implicazioni delle scelte sui cittadini e sulle generazioni future. La sfida è culturale oltre che tecnica, e richiede un salto significativo nella formazione della classe dirigente, affinché dati diventino strumento di progresso e non fonte di discriminazioni o asimmetrie sociali.

In un contesto in cui la digitalizzazione permea ogni aspetto della vita pubblica e privata, la protezione dei dati personali rimane un pilastro fondamentale per la tutela dei diritti dei cittadini e per il buon funzionamento della democrazia.

Consapevolezza, educazione digitale e governance *responsabile diventano strumenti essenziali per trasformare l'innovazione tecnologica in un'opportunità concreta, rendendo i servizi pubblici più sicuri, trasparenti e inclusivi.*

Conclusioni

II futuro digitale richiede un approccio integrato: cittadini informati e partecipi. Pubblica amministrazione attenta ai rischi e alle potenzialità, imprese e istituzioni capaci di innovare nel rispetto dei principi fondamentali di protezione dei dati. Solo così l'intelligenza artificiale e le nuove tecnologie potranno diventare veri alleati, contribuendo a costruire una società digitale in cui progresso, fiducia e responsabilità camminano di pari passo.

Social media online la guida aggiornata del Garante privacy

Sei sicuro che le foto e le informazioni che pubblichi ti piaceranno anche tra qualche anno? Da quanto tempo non verifichi le impostazioni privacy dei tuoi profili *social*? Hai mai provato a navigare insieme a tuoi figli? Sono alcuni degli spunti di riflessione che il Garante per la protezione dei dati personali rivolge a minori, genitori e utenti nella nuova edizione della sua **guida "*Social privacy*. Come tutelarsi nell'era dei *social media* "**.

I *social network* sono il luogo in cui non esistono barriere tra la vita digitale e quella reale: quello che succede *online* - ricorda l'Autorità - ha sempre più spesso impatto fuori da Internet, nel quotidiano e nei rapporti con gli altri. I *social* rendono più semplici i contatti, favoriscono lo scambio di informazioni con un numero enorme di persone, permettono di esprimere idee, passioni o talenti, ma amplificano allo stesso tempo i rischi di un utilizzo improprio o fraudolento dei dati personali, esponendo gli utenti a furti di identità, abusi, danni della reputazione, informazioni non verificate o vere e proprie *fake news*.

Proprio con l'obiettivo di aumentare la consapevolezza dei giovani, e degli adulti, e far conoscere i diritti di ognuno e gli strumenti di tutela proposti dal Garante, l'Autorità ha aggiornato questa guida ai *social media* mantenendo la struttura agile che ne ha favorito la diffusione e il facile utilizzo, grazie anche a una serie di "avvisi ai naviganti" e consigli di utilizzo.